Responses to Advance Questions
For Mr. Arthur L. Money

1. Defense Reforms

More than a decade has passed since the enactment of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 and the special operations reforms. As part of your confirmation in November 1995, you affirmed your support for full implementation of these defense reforms. In addition, you assured the committee that one of your top priorities would be to continue the reform activities under way in the Air Force and the Department of Defense especially with regard to streamlining the acquisition process and strengthening program management and execution.

A. Do you still support full implementation of the Goldwater-Nichols and special operations reforms?

ANS: Yes, I continue whole-heartedly to support full implementation of the Goldwater-Nichols and special operations reforms.

B. Please provide specific examples of initiatives you implemented while serving as the Assistant Secretary of the Air Force for Acquisition.

ANS: The following are examples of initiatives implemented during my tenure as Assistant Secretary of the Air Force for Acquisition. Under my leadership, $30 Billion in program savings and/or cost avoidance were achieved through implementation of an 11 point Lightning Bolt Program. The program consisted of the following elements:

- A Request for Proposal (RFP) Support Team – which resulted in the reduction of the average size of RFPs by 50%, emphasized the use of Statements of Objectives that allow industry to respond with time and cost-saving solutions, and reduced contract data requirements.
- Establishment of a standing Acquisition Strategy Panel – resulting in a predetermined total program life-cycle strategy.
- A Program Office "SlimFast" plan -- resulting in fewer US government personnel in each program office.
- Cancellation of all local acquisition policies – resulting in centralization of policy at Air Force Headquarters with decentralized execution; resulting in consistent processes across the Air Force.
- Reinvention of the program approval process – shortened and improved efficiency of the approval process.
- Enhancing the role of contractor past performance as a factor in the Source Selection process – resulting in improved performance on all existing contracts.
- Creation of a single approval document, Single Acquisition Management Plan (SAMP) compared to multiple documents required previously – previous requirement resulted in 10,000 pages compared to 50 pages for the SAMP.
- Establishment of metrics to monitor acquisition reform progress – put output metrics

into system performance.
- Increased Acquisition training for all personnel.
- Reduction of acquisition cycle time, which shortened the time from concept development to delivery of systems.
- Introduction of Acquisition reform at laboratories – put labs under the same acquisition system

The goals of the Congress in enacting these defense reforms, as reflected in Section 3 of the Goldwater-Nichols Department of Defense Reorganization Act, can be summarized as strengthening civilian control; improving military advice; placing clear responsibility on the combatant commanders for the accomplishment of their missions; ensuring the authority of the combatant commanders is commensurate with their responsibility; increasing attention to the formulation of strategy and to contingency p1anning; providing for more efficient use of defense resources; and enhancing the effectiveness at mi1itary operations and improving the management and administration of the Department of Defense.

C. Do you agree with these goals?

ANS: Yes

Recently, there have been articles, which indicate an interest within the Department of Defense in modifying Goldwater-Nichols in light of the changing environment and possible revisions to the national strategy.

D. Do you anticipate that legislative proposals to amend Goldwater-Nichols may be appropriate? If so, what areas do you believe it might be appropriate to address in these proposals?

ANS: The Department is continuing to examine ways to better support the goals of the reform in light of our ever-changing environment. I believe that the Goldwater-Nichols legislation is still very valid and does not need to have major changes.

2. Relationships

If confirmed, what will be your relationship with:

A. The Secretary of Defense

ANS: If confirmed, I will function as DoD Chief Information Officer (CIO) and as the principal staff assistant and advisor to the Secretary of Defense for all C3I matters. In particular I will be responsible for providing policy, guidance and oversight for C3I functions including:

- Command, control, communications, intelligence, surveillance, and reconnaissance sensors;
- Information technology, management, operations, assurance, and superiority;
- Electronic commerce and business process reform;
- Intelligence and counterintelligence;
- Personnel, industrial, and classification security;
- Frequency-spectrum management;
- Space systems; and,
- Critical infrastructure protection.

B. The Deputy Secretary of Defense

ANS: If confirmed, my relationship with the Deputy Secretary of Defense will be the same as that described above in relation to the Secretary of Defense.

C. The Under Secretaries of Defense

ANS: If confirmed, my relationship with the Under Secretaries of Defense and other senior officials of the Department will be based on the role of each principal official within the Department of Defense with respect to my functions as described above in the relationship to the Secretary of Defense. With respect to acquisition of C3ISR and space systems, I will report to the Deputy Secretary of Defense through the Under Secretary of Defense for Acquisition and Technology.

D. The Assistant Secretary of Defense for Special Operations and Low Intensity Conflict

ANS: If confirmed, my relationship with the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict will be similar to that described below in relation to the other Assistant Secretaries of Defense. In particular, I will coordinate the Psychological Operations aspect of Information Operations with the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict.

E. The other Assistant Secretaries of Defense

ANS: If confirmed, my relationship with the Assistant Secretaries of Defense and other

senior officials of the Department will be based on the role of each principal official within the Department of Defense with respect to my functions as described above in the relationship to the Secretary of Defense.

F. The General Counsel of the Department of Defense

ANS: If confirmed, my relationship with the General Counsel will be based on my role as principal staff assistant to the Secretary of Defense for C3I matters and as CIO and I will consult with the General Counsel on all CIO, C3ISR and space matters meriting legal review.

G. The Chairman of the Joint Chiefs of Staff

ANS: If confirmed, I will continue to coordinate and exchange information with the Chairman of the Joint Chiefs of Staff on C3I matters and on information resources management matters, appropriate, to ensure all policy and guidance issues under my cognizance are supportive of the Commanders-in-Chief and Military Services.

H. The Commander-in-Chief United States Special Operations Command

ANS: If confirmed, my relationship with the Commander-in-Chief United States Special Operations Command will be based on my role as the CIO and as principal staff assistant to the Secretary of Defense for C3I functions, and I will coordinate and exchange information with the Commander-in-Chief United States Special Operations Command and Assistant Secretary of Defense for Special Operations and Low Intensity Conflict on matters of mutual interest to ensure policy and guidance matters under my cognizance are supportive of the CINC's roles and missions.

I. The regional combatant CINCS

ANS: If confirmed, my relationship with the regional combatant CINCs will be based on my role as principal staff assistant to the Secretary of Defense for C3I functions and as CIO, and I will coordinate and exchange information with the CINCs on matters of mutual interest to ensure C3I and information resources management policy and guidance are supportive of the CINCs' roles and missions.

J. The Director of the Defense Intelligence Agency

ANS: If confirmed as the Secretary of Defense's principal staff assistant for C3I functions, I will exercise authority, direction and control over the Director, Defense Intelligence Agency.

K. The Director of the National Imagery and Mapping Agency

ANS: If confirmed as the Secretary of Defense's principal staff assistant for C3I functions, I will exercise authority, direction and control over the Director, National

Imagery and Mapping Agency, working closely in consultation with the Director of Central Intelligence, as appropriate.

L. The Director of the National Security Agency

ANS: If confirmed as the Secretary of Defense's principal assistant for C3I functions, I will exercise authority, direction and control over the Director, National Security Agency, working closely in consultation with the Director of Central Intelligence, as appropriate.

3. Duties

Section 138 of Title 10, United States Code, provides that the Assistant Secretaries of Defense shall perform such duties and exercise such powers as the Secretary of Defense may prescribe.

A. Assuming you are confirmed, what duties do you expect that Secretary Cohen will prescribe for you?

ANS: If confirmed, my principal duty as the Assistant Secretary of Defense for Command, Control, Communications and Intelligence will be to exercise policy, guidance, planning, resource management, and program oversight of these assigned activities within the Department of Defense. These activities are in part described above.

B. If confirmed, will you report directly to the Deputy Secretary of Defense and Secretary of Defense?

ANS: Yes

C. If confirmed, will you represent the Secretary in all deliberations with the Director of Central Intelligence with regard to the National Foreign Intelligence Program?

ANS: Yes

D. If confirmed, what duties and responsibilities do you anticipate being assigned as the Chief Information Officer of the Department of Defense?

ANS: I will be assigned those responsibilities that all Federal Agency CIOs are given under the provisions of the Clinger-Cohen Act (Section 5125). With regard to DoD, this would include being the Secretary's principal staff assistant for all information technology, information resources management and information management matters. As such I would provide advice and assistance to him and other DoD senior management personnel to ensure that information technology is acquired and information resources are managed in a manner that implements the provisions of the Act and the priorities established by the Secretary.

In addition, I would anticipate having those duties assigned and authorities delegated to the DoD CIO by the Secretary in his memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," dated June 2, 1997. In essence, these are the duties and responsibilities assigned to the head of each Federal Agency in the Act.

Finally, I would have those additional responsibilities given to the DoD CIO in the FY 1999 National Defense Authorization Act. Specifically, I would review and provide recommendations to the Secretary of Defense on DoD budget requests for, and

ensure the interoperability of, the information technology and national security systems throughout the DoD, ensure that information technology and national security systems standards applicable throughout the Department are prescribed, and provide for the elimination of duplicative information technology and national security systems within and between the Military Departments and Defense Agencies.

4. Qualifications

If confirmed, you will be entering this important position at a time of concern about the adequacy of the budget, force levels and readiness of our forces.

A. What background and experience do you have that you believe qualifies you for this position?

ANS: I have more than 34 years of management and engineering experience with the defense electronics and intelligence industry in the design and development of intelligence collection analysis capabilities and airborne tactical reconnaissance systems. I have also served as the Assistant Secretary of the Air Force for Acquisition for two years, and most recently (since February 1998) I have been serving as the Senior Civilian Official for the Office of the Assistant Secretary of the Defense for Command, Control, Communications, and Intelligence (OASD(C3I), as well as the DoD Chief Information Officer.

At the direction of the Deputy Secretary of Defense and during my tenure as the Senior Civilian Official, I have established a new, revitalized organization focused on the broader and increasing C3I mission in today's environment. The new C3I organization, which includes day-to-day reporting of DIA, DISA, DSS, NIMA, NRO, and NSA, was formally established in June 1998, and is designed to address Information Superiority in its entirety. I created ten goals to focus our attention on truly achieving Information Superiority:

1. Ensure Continuity of Mission Essential DoD Operations Despite Y2K Disruptions
2. Implement Effective Programs for Information Assurance and Critical Infrastructure Protection
3. Build a Coherent Global Network Based on Efficient and Effective DoD Information Architectures and Procedures
4. Plan and Implement Joint and Combined End-to-End C3ISR and Space Integration
5. Establish a Knowledge-Based Workforce Within DoD
6. Establish Policies and Budget Priorities That Will Lead to the Reinvention of Intelligence for the 21st Century
7. Revise Policies for Information Operations, Security and Counter-Intelligence
8. Establish Electronic Commerce and Business Process Change Throughout the Functional Areas of DoD
9. Develop an Advance Technology Plan for Information Superiority
10. Transform OASD(C3I) into a Nurturing, Caring Organization that Serves as a Model Team in Attaining its Goals

Both the Secretary and Deputy Secretary have approved the ten goals, and we've made significant progress on each one over the last year.

B. Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Assistant Secretary of Defense for Command,

Control, Communications and Intelligence?

ANS: I believe I am professionally and technically prepared to assume the duties of the Assistant Secretary of the Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). I expect to be aided in my duties by the strong management team that currently exists within the Department and the C3Istaff.

I believe it is critical that we create and retain a much more robust knowledge-based workforce within DoD to meet the increasing information superiority challenges we face. Additionally, I believe it is imperative that both my management team and I stay abreast of industry's information technology advancements so that they may be applied effectively to the accomplishment of information superiority.

5. Position Title

Section 902 of the National Defense Authorization Act for Fiscal Year 1999 repealed the statutory requirement to have an Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The conference report accompanying that act also endorsed changing the name from C31 to Space and Information Superiority to more appropriately describe the duties of the restructured organization.

Why has the Department not yet changed the name?

ANS: I am informed that, upon closer examination of the functions assigned to the ASD(C3I), the Department came to the conclusion that a name change to Space and Information Superiority would diminish our core missions of command and control, communications, and intelligence. The functions of C3I are carried out on land, on the sea, in the air, and in space; it would diminish the value of the other critical areas to highlight only one of these locations. Furthermore, the execution of our core missions accomplishes information superiority.

6. Information Superiority

You often describe your responsibility in OSD as "information superiority."

Describe your vision of information superiority for DOD, including the principal impediments facing the Department.

ANS: DoD is currently embarked upon a journey that will transform the Force of the 21st Century. Information Superiority is on the critical path to achieving this transformation. The Defense Planning Guidance and Joint Publication 3-13 describe Information Superiority in terms of what we need to achieve it – that is, the "ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and / or denying an adversary's ability to do the same." The net result is a state in which we are more aware, indeed more knowledgeable, about the situation than our adversaries.

The concept of Information Superiority is equally applicable to both "sides" of the DoD--the business side and the warfighting side. The Revolution in Military Affairs will build upon the lessons learned in the Revolution in Business Affairs, adapting the concept of Information Superiority to the military domain. This will transform military operations into Network Centric Warfare, increasing the tempo of operations, the speed of command, and, as a result, achieve greater lethality with increased survivability. The net result will be an opportunity for quicker and more decisive victories, using less "tail" (support) and more "tooth" (warfighting capability).

Achieving Information Superiority is not simply a matter of acquiring advanced information technology. As we are increasingly becoming more dependent on a fragile and vulnerable information infrastructure ("infostructure"), interoperability problems persist within each of the Services and in the Joint arena. The increasing importance of coalition operations still is not adequately mirrored by an increased effort to achieve coalition interoperability. In short, there is a disconnect between the future concepts being developed and the planned reality in the same time frame. Finally, there are significant impediments to progress in the way we fund, design, and acquire our infostructure that result in interoperability problems and security risks.

In focusing on achieving Information Superiority for the warfighter, if confirmed I will continue to pursue the accomplishment of these ten goals for C3I which are described above under my qualifications. These goals are not just my goals, but in reality they need to become broadly shared goals. It is essential that we work together to make progress, assess our progress regularly, and find ways to make even more progress. I am committed to the achievement of these goals and want to partner with others in DoD and in Congress to expedite progress.

7. Worldwide Communications Capabilities

A July 1997 report by the Department of Defense Inspector General entitled "Communications Capability with The Department of Defense to Support Two Major Regional Conflicts Nearly Simultaneously" identified significant deficiencies in the Department of Defense satellite communications capacity and other communications systems.

A. Please, provide an update on actions taken or planned to address the problems identified in the July 1997 Inspector General report.

ANS: A great deal has changed since, and in response to, the July 1997 Inspector General (IG) report. DoD has established an effective, affordable modernization plan for its satellite communications systems based on a comprehensive analysis of all its future requirements, and has revised the process for allocating this limited resource to meet warfighting needs.

In August 1996, the Department approved its future Military Satellite Communications (MILSATCOM) architecture that aligned military requirements into three core functional segments: protected, wideband, and mobile communications. The intent of this alignment was to move all users who required protected communications (e.g., front-line tactical forces and strategic nuclear forces) to a single military-unique system, current Military Strategic Tactical and Relay (MILSTAR) and its Advanced Extremely High Frequency (EHF) follow-on program launching in 2006. This move allows the two other segments, wideband and mobile, to be as commercial-like as possible to best leverage the technology and investments being made in the exploding commercial satellite communications market.

Even as the IG report was being written, key questions raised in the report were being answered by the Transition Working Group led by the then Deputy Under Secretary of Defense for Space (now part of the C3I organization) and the Senior Warfighter Forum led by the Deputy CINC USSPACECOM. These groups identified the correct mix of capacity for each segment based on a detailed assessment of future warfighting needs given our overall fixed budget. Using this information, the groups outlined system acquisition details, including the schedules for replacing our current generation of satellites. One of the key refinements in the Transition Plan approved in August 1997 was the establishment of the Wideband Gapfiller program that would accelerate deployment of a more than five-fold increase in wideband capacity to the warfighter. The Wideband Gapfiller will launch in 2004, sooner than the previously envisioned Advanced Wideband System (previously launching in 2006, now scheduled for 2008). The Wideband Gapfiller system is a commercial-like system owned by the government that consolidates and increases the capacity of the current Defense Satellite Communications System (DSCS) X-band and Global Broadcast Service systems and adds a new two-way Ka-band capability.

Despite significant capacity increases in all its planned next generation systems,

our analysis tells us that with our fixed budget the Department will still fall short of the needed satellite capacity. DoD's recent experience in the Balkans confirms the ever-increasing information requirements of modern warfare. To mitigate expected future shortfalls, the Department has taken steps to more efficiently use our existing resources. The deployment of Demand Assigned Multiple Access capability allows more users to rapidly access resources for only the period of time needed. The Defense Information Systems Network is deploying high-capacity fiber optic cable around the world where possible. DoD is adding satellite gateways to connect this terrestrial infrastructure with deployed warfighters to make efficient use of our space communications assets. In addition, bandwidth efficient modems are making the most use of current wideband resources. The Department is also using commercial systems to augment military-owned and operated systems as needed for surge and niche capacity. We are overhauling the Commercial Satellite Communication Initiative program to provide more responsive end-to-end commercial service. We have added one Mobile Satellite Service provider as a secure augmentation to the Department's current Ultra High Frequency (UHF) Follow-On mobile satellite system, and we are taking steps to secure other commercial providers. Finally, DoD continues to explore new promising technologies (e.g., Unmanned Aerial Vehicles communications nodes, laser communications, and spectrum reuse techniques, as well as fiber optic media) for integration into our future plans as appropriate.

To help DoD better manage our limited satellite communications resources, we have revised and updated our management strategy in the new Chairman of the Joint Chiefs of Staff Instruction. Among the many processes addressed in this document is the allocation of limited satellite capacity to ensure the right communication to the right person at the right time based on military needs.

Furthermore, the Department is working with our allies to ensure they understand the evolving threats and our implementation plans. The objective is to achieve interoperability. It is our goal that we have a shared vision of the doctrine and concept of operations needed to successfully engage future adversaries, or to conduct peacekeeping operations.

This will ensure the Department is on a course to provide future warfighters with a robust mix of communications to meet their missions. If confirmed, I am committed to deploying a coherent global network based on efficient and effective DoD information architectures and procedures within the Department's budget.

Other information received by the Committee reinforces these findings and indicates that there may be significant deficiencies associated with communications systems of Department of Defense aircraft supporting senior military personnel, including the war fighting CINCs.

B. Describe the deficiencies associated with these aircraft and your plans for addressing them.

ANS: The Department of Defense provides a significant share of the communication capability required by our nation's leaders, both military and political. Our requirement is essentially to provide immediate, totally reliable, secure communications and information between our national leaders seven days a week, 24 hours a day, around the globe, including in aircraft while these leaders are traveling.

Challenges and Solutions: The Department is currently undertaking an extensive effort to identify and correct deficiencies.

Aircraft: Within the last year, 22 problem areas were identified onboard these aircraft. Eight of these problems have been corrected. Six problems resulted from inaccurate, site-specific equipment information, and are currently being corrected with revised procedures. The remaining eight items are under review, with the expectation that they will be fixed in the near future.

Ground Infrastructure: There are also problems with the supporting ground infrastructure used to connect aircraft to the public telephone system. The majority of communications between leaders passes through an aging system located within the Washington, D.C. area. An extensive technical and operational examination of this system is being conducted by the Defense Information Systems Agency, with help from the White House Communications Agency, to determine specific shortfalls and enhancements.

Interoperability: Because of the many different aircraft configurations and multi-agency customers, an ongoing problem is ensuring interoperability. This includes compatibility between the various aircraft and the "office" or CINC command systems, interoperability among the many different types of aircraft, and interoperability between the aircraft and a wide variety of ground links (U.S. and foreign owned, commercial and military equipment). The Department is currently establishing the interagency Senior Leadership Travel Communication System (SLTCS) Executive Management Board to monitor the performance of all senior leadership communication systems, both air and ground; and to coordinate operational requirements of all users. Once fully developed the SLTCS process will determine and maintain system configuration control, proactively measure system performance to detect problems before they become critical, coordinate procedures, and maintain the technical and operational roadmaps to ensure reliable and interoperable communications in the future.

If confirmed, I will remain personally committed to ensuring that our military and civilian leaders, while onboard DOD aircraft, have the necessary information and communications capability to conduct their duties.

8. Responsibilities in Space

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence has been assigned the lead within the Office of the Secretary of Defense for military space matters.

A. What have you accomplished as Senior Civilian Official, and what do you plan to do if confirmed as Assistant Secretary, to ensure that space oversight not be overshadowed by the information superiority aspects of your duties?

ANS: I fully recognize that our ability to access and utilize space is a vital national interest. The priority I will assign to the space policy and oversight responsibilities I will have if confirmed as the ASD (C3I) will be fully integrated with, and complementary and synergistic with the information superiority aspects of my duties. Space-based resources provide significant capabilities to collect and disseminate C3ISR support to U.S. military forces and the National Command Authority. Access to and use of space will help enable the United States to establish and sustain the battlespace dominance and information superiority necessary to achieve success in military operations.

The following are several major space initiatives and accomplishments that have occurred during my leadership/tenure as the Senior Civilian Official:

- C3I formulated revision of DoD Space Policy that reflects new priorities and establishes a comprehensive framework that will help to articulate the need for capabilities, guide the allocation of resources, and direct programmatic activities.

- C3I formulated and led the execution of a space control strategy, presented to the Strategic Forces Subcommittee by the Deputy Secretary earlier this year, that implements National and DoD policy and initiates technology readiness activities to enhance the surveillance, protection, prevention, and negation missions. In this regard, DoD has also initiated a broad area review of the Department's space control activities, begun development of a comprehensive space control technology roadmap that will unite space control research and development programs across the Department, and created a unique budget line for space control technology to help monitor key activities.

- C3I led the successful effort to define licensing criteria for commercial hyperspectral imagery systems, finalized DoD policy guidance on the interruption of commercial remote sensing space operations to protect U.S. national security, assisted NOAA in its development of a commercial remote sensing enforcement plan, and helped represent the U.S. Government in international consultations on remote sensing policy with other supplier nations.

- Internationally, C3I concluded an independent assessment of US-French space cooperation as well as joint analysis of C4ISR and space interoperability needs and Report to the Secretary of Defense and French Defense Minister that led to the

creation of a bilateral C4ISR & Space Interoperability Working Group. We also have taken a leadership role in the pursuit of international agreements on space cooperation with Italy, Spain, and Japan.

- C3I conducted the National Launch Capabilities Study, a comprehensive review and assessment of future launch requirements, launch and range infrastructure, and future management of DoD space launch capabilities.

- The Interagency Global Positioning System (GPS) Executive Board, of which I have acted as a co-chair, has led the effort to analyze alternatives and set in motion the process for introducing the third civil GPS signal. In this day of scarce spectrum resources, securing spectrum for new signals is becoming increasingly challenging. While this task is not completed yet, it has been gratifying to see military and civil elements of the government cooperating to identify the best approach to the new civil signal from an overall national perspective.

B. Please describe the most significant challenges facing the Department of Defense and the intelligence community in providing space support to the war fighter.

ANS: Maintaining robust constellations of space-based systems will always be a significant challenge. The pressures of constrained resources, premature on-orbit failures, effects of space weather, and changes in the threat make constellation sustainment difficult. Sustaining this critical infrastructure and, at the same time, evolving other air, sea, and ground based missions to space where they can be more effectively accomplished takes more resources than we have currently allocated. In many cases we are not technology driven, we are resource driven. However, we have been successful at pursuing both the Discoverer II program (Moving Target Indicator) and the Space Based Laser demonstration as examples of the direction our future in space may take us. We have continued the space control initiatives that Congress directed in the FY99 defense bills with FYDP funding requests in our 2000 President's Budget.

As warfighter requirements evolve, the technology challenges become enormous. As we have seen with the SBIRS Low system, modern space systems, required to meet complex and challenging threats, are very technically complicated. Not only are the sensors challenging but the supporting systems are as well. For example, the requirement for inter-constellation communications and cooperation is a significant step from where our traditional systems have operated. The requirements for large, precision optics is growing while the emphasis on smaller, lighter, cheaper satellites are pushing well past current limits of technology. Deployable and inflatable optical concepts are under development, but solutions remain well into the future. As you can see, technology development is one of the significant keys to meeting future challenges.

As daunting a challenge as the pure collection of information is, the integration and dissemination of the data in a timely manner, sensor-to-shooter, remains the ever-present task. Getting the right information to the person at the right time will always be the ultimate objective.

GPS poses a significant challenge for we must find ways to accelerate the availability of critical enhancements needed to improve both military and civil utility of the current system so that we do not lose the lead we have obtained globally in this area. We are currently evaluating potential alternatives and should have a plan in the near future. In the area of funding our fundamental approach is based on the premise that a purely military requirement ought to be funded by the DoD and a purely civil requirement should be funded by the civil agencies. Through the Interagency GPS Executive Board, we have developed military/civil equitable cost-sharing arrangements. However, problems continue with the budgeting process when either the civil or military contributions of the cost-sharing arrangements fall short.

9. Funding Challenges

During your testimony before the Emerging Threats and Capabilities Subcommittee on March 16, 1999, you indicated that the Department of Defense faced significant funding shortfalls in the area of information assurance in fiscal year 2000 and in the FYDP.

Will you seek increases in funding in this area as part of future budget preparations?

ANS: Yes.
Given the risks and the fact that weakness in any portion of the Defense Information Infrastructure pose a threat to the operational readiness of all Components, the Department is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information and the protection of its information infrastructure. These five elements collectively provide what we refer to as information assurance (IA). RDT&E is needed to ensure that security features keep pace with the tremendous bandwidth and speed increases occurring in our information architectures. Additional funding would be used to develop very high-speed encryption devices; electronic re-keying capabilities; and advanced key management techniques. Procurement funds are needed for Secure Terminal Equipment to replace aging and outdated STU-III equipment and to leverage capabilities offered by digital network technology. RDT&E is required for Secure Wireless Communications and for implementing compatible security over the growing and emerging wireless infrastructure to provide the capability for joint forces to use whatever wireless services are available in a given region of the world. Procurement funds are needed for the development/purchase of tools for real-time detection, collection, and analysis of attack sensing and warning data.

The Department needs to accelerate greatly implementation of a Public Key Infrastructure (PKI) across the Department to achieve a solid foundation for public key-enabled security services and to ensure interoperability throughout the Department. The DoD PKI will be an important component supporting the IA capabilities of the Department. DoD has issued aggressive policies to spur the acquisition and use of PKI-enabled services. These policies are designed to place the PKI-enabled services within a Defense-in-Depth context that takes advantage of other layers of protection. Acceleration of funds is needed to move quickly to a hardware token-based PKI, and to field rapidly the associated infrastructure components and applications necessary to support it. For example: fielding an infrastructure for local registration authorities and certificate authorities across the Department; greatly accelerating the schedule for hardware-related cards and readers; conducting training and fielding software associated with registration, certificate authorities, and digital signatures; implementing web server access controls; enhancing electronic mail capabilities; and modifying existing applications with PKI-enabling capabilities. We believe that this accelerated migration is critical in light of the expanding threat environment in which we conduct our operations.

Increased funding for information technology (IT) training is critical if the

Department of Defense is to achieve information superiority. A corps of appropriately trained and experienced IT professionals is the most critical component in protecting the Department's information resources against modern day cyber attacks. Individuals using, administering, and maintaining these systems must follow prescribed protective procedures, and know how to operate the equipment designed to mitigate these threats. A strong incentive program is required to enable, acquire, and retain a cadre of highly skilled IT professionals, both uniformed and civilian. The Department's IT specialists represent a world-class force of IT warriors who have proven themselves enormously capable in meeting IT challenges. However, these specialists also possess skills that are in great demand in the market place, so we must be able to offer highly regarded incentive packages. To meet the challenges of the future the Department must have coherent programs, with sufficient resources, to compete with commercial industry in order to attract and retain the very best.

10. Information Assurance

Section 1047 of S. 1059, the Senate-passed version of the FY 2000 Defense Authorization Act, would require establishment of an Information Assurance Initiative, including the creation of an Information Assurance Testbed.

Please provide your views on this provision.

ANS: I support the creation of an Information Assurance (IA) testbed. Such a testbed is fully consistent with initiatives ongoing within the Department today designed to support the Department's operational readiness requirements and its IA vision, goals, and objectives. The Defense-wide Information Assurance Program (DIAP) was created in January 1998 to be the Office of the Secretary of Defense's mechanism to plan, monitor, coordinate, and integrate IA activities. Since its creation, the DIAP has improved the coordination of DoD IA efforts appropriate to the shared risk environment in which the Department and supporting entities must operate. In a networked environment, a risk accepted by one becomes a risk imposed on all. The DIAP is working to ensure the Department maximizes the return on its IA investments.

The establishment of an IA test-bed will allow for the development and conduct of information warfare simulations, war-games, exercises, and other activities designed to better inform and prepare the Department for responses to information warfare threats. Further, it will allow for the development of essential design and operational testing measures and the ability to assess the conformance of IA-enabled products and composed systems against such measures.

C3I is working very closely with the various committees under the Federal Chief Information Officer's Council, the National Security Telecommunications and Information Systems Security Committee, and Critical Infrastructure Assurance Office to ensure a cross-flow of information between the Department and the agencies and organizations that we depend upon for our daily operations. Through these various channels, we have already orchestrated a number of exercises and experiments to improve our infrastructure and information assurance posture and we will certainly strive to strengthen, focus, and improve those efforts in the coming year.

11. Smart Card Technology

Section 347 of S. 1059 requires an assessment of the use of smart card technology as the Public Key Infrastructure authentication device for DOD.

Please provide your views on this matter.

ANS: I believe that smart cards offer tremendous potential to support multiple application and multiple technology solutions for business and military needs including use as PKI tokens. We are considering placing keys onto smart cards and making them "Common Access Cards" which may be used for both building and facility access as well as computer and network access. We are beginning a common access card pilot test in the next two months to prove the concept of a common access card. Additionally, one Defense Agency has been successfully using smart cards as PKI tokens for over a year now.

Although smart cards have tremendous potential for PKI applications, I believe that it is premature to make a decision now to limit PKI tokens to smart cards only. Technology is emerging and evolving rapidly in this area. There is no clear defacto industry standard for PKI hardware tokens. While we certainly will employ smart card technology to address near-term needs, we must remain flexible to allow for migration to other solutions if industry standards dictate this. I want to allow for consideration of other technologies, if they are operationally effective, cost effective and easier to implement. In any case, however, I envision that eventually DoD will employ a limited set of hardware token solutions.

Recognizing that PKI technology is still immature in the marketplace and changing rapidly, DoD's strategy is to pursue early adoption of technology and services, actively participate with industry to obtain the detailed technical understanding needed to specify requirements fully, resolve standard issues, and accelerate industry-wide convergence to purely a standards-based, interoperable capability which is not dependent on vendor-specific capabilities or technologies. Balanced with the need to provide appropriate levels of security now, is our need to keep pace with the technological rollover inherent with commercial products and standards.

We have categorized PKI keys and certificates into levels of assurance. For those instances that require high levels of assurance, but do not involve classified information, we have issued policy that the PKI keys must be located on a hardware token. Under current technology, examples of hardware tokens are Smart Cards, PC Cards, and in the future, possibly Universal Serial Bus tokens. The protection of classified information also will require hardware tokens, but only those certified by the National Security Agency will be used for that level of security.

12. Intelligence Programs

With the development of increasingly advanced information technologies, and the evolving role of intelligence in support of military forces and operations, the current intelligence categories -- NFIP, JMIP and TIARA -- appear to be increasingly blurred.

A. In your view, should these categories be reevaluated?

ANS: I believe we should retain this structure as it provides the necessary focus for each customer to state needs within a resource/programmatic context to ensure that they are being identified, prioritized, and addressed appropriately.

Each of the program components mentioned -- NFIP, JMIP, and TIARA -- has a primary focus in support of customer requirements: NFIP on the national customers, JMIP on DoD's joint military requirements, and TIARA on the organic tactical needs of the fighting forces. For each element, the primary customers make an initial projection of how resources can be best allocated to meet their needs. Together, they form the end-to-end structure needed for intelligence support.

B. Do you believe that the current management and budgeting oversight of these programs between the Secretary of Defense and the Director of Central Intelligence is adequate?

ANS: Yes. The process used today is a major improvement over how programs were developed prior to 1992. However, we will continue to improve the overall process of integration across all customers relying on intelligence input.

C. If not, what changes would you recommend?

ANS: If confirmed I would recommend creation of a mechanism to gain visibility of all dollars associated with information superiority, to include intelligence. Furthermore, if confirmed, I would continue supporting the creation of an integrated requirements framework and joint strategic planning process – managed by the DCI and the Department of Defense – that provides linkages between Service, Agency, and Departmental assets. Key to success will be refining the Intelligence Community's program and budget formulation process to improve cross program decisions, and relate intelligence performance to national security. This is also critical to DoD's goal to reinvent Intelligence for the 21st Century and provide critical information to the warfighter. If confirmed, I will continue to improve these processes to achieve the results our warfighters deserve.

D. In your view, do the Office of the Secretary of Defense and the Joint Staff have sufficient influence over major programmatic and architecture decisions within the National Foreign Intelligence Program?

ANS: Yes. All major programmatic decisions are reviewed through the Joint Requirements Oversight Council (JROC) process. Chaired by the Vice-Chairman of the Joint Chiefs of Staff, the JROC brings into play all the key military players of the Department to determine needs versus the resources required. This has resulted in major improvements in recent years in decisions to meet military customer requirements.

Recent events in Kosovo illustrated continuing deficiencies in the area of map development, production and dissemination.

E. Provide your assessment of the scope of this problem and the adequacy of plans for addressing it.

ANS: As for the scope of improvement to mapping development, production, and dissemination with respect to Kosovo, lessons learned and after-action reports are being developed by all agencies involved in a primary or support role. The findings will be reviewed and appropriate actions will be taken to improve all areas found to be deficient. If confirmed, I intend to discuss this issue further after the lessons-learned and after-action assessment is complete.

F. Please provide your assessment of current airborne reconnaissance capabilities and programs, including needed improvements to operational systems, deficiencies in ongoing development and acquisition program and any proposed changes in management or organizational structure.

ANS: The Department has been highly successful in modernizing and increasing our Intelligence, Surveillance, and Reconnaissance (ISR) force structure since the Gulf War. At the same time, we have found the "peacetime" OPTEMPO for these assets is demanding critical deconfliction efforts between competing CINCs' taskings, as well as placing significant burdens on the people who operate them. Our ISR platforms have become workhorses for worldwide contingency operations such as Bosnia and Kosovo.

The success of DoD's manned reconnaissance programs has been enhanced by several initiatives, which will extend the viability of these assets well into the next century:

- DoD has completed a major U-2 fleet overhaul including engines, rewiring, and sensor suites. Our final re-engined U-2S aircraft was delivered in December 1998 giving greater payload, range, and altitude performance.
- The RC-135 RIVET JOINT fleet is expanding from 14 to 16 aircraft this year; the COBRA BALL, from two to three aircraft increasing available platforms for worldwide Measurement and Signature Intelligence tasking. The entire RC-135 fleet is now fully funded for re-engineering and this must stay on track.
- To ensure EP-3 connectivity and interoperability, a signals' processing infrastructure will be installed compliant with the Joint Airborne SIGINT Architecture. Funding has been identified to replace an aircraft destroyed in a 1997 mishap, bringing the

fleet back to 12 aircraft.

- The Predator Unmanned Aerial Vehicle is the first Advanced Concept Technology Demonstration to transition to a formal acquisition program. Five of 12 systems have been delivered and the first baseline production system will include improved communications relays, de-icing capability and a new engine. Earlier systems must be retrofitted to this baseline
- The Joint SIGINT Avionics Family (JSAF), a key part of JASA, will be employed on our ISR aircraft and is currently undergoing flight test operations.
- Distributed Common Ground Systems will be interoperable with airborne sensors allowing seamless fusion of multi-intelligence information into the joint C4I environment.

Today's environment also presents us with several challenges:

- Force restructuring and a more unpredictable world situation have led to increased demand for US military forces. Nowhere has this been felt more than in our low-density high demand reconnaissance forces, especially during the Kosovo conflict. To alleviate this stress, we must field more reconnaissance assets.
- DoD also continues to monitor the health of our ISR work force to discern ways to ease deployment and other pressures so we can better retain experience.
- A comprehensive imagery modernization plan to improve the balance between collection and Tasking, Processing, Exploitation, and Dissemination (TPED) to maximize capability and size the multi-intelligence ISR TPED envisioned by Joint Vision 2010.

Despite success, DoD does have development deficiencies to address:

- From the High Altitude Endurance UAV ACTD experience, we learned to assess an ACTD before completion. DarkStar demonstrated only limited flight performance while surpassing the stated unit flyaway price and therefore was not considered worth the investment.
- The Joint Tactical UAV (TUAV) Program indicated that one TUAV couldn't satisfy the needs of all the services. The OUTRIDER ACTD demonstrated it could not meet the Navy's range and endurance requirement nor the Army's endurance and short-field landing requirement.
- We are applying Predator ACTD transition lessons to Global Hawk, design-to-cost with a military utility demonstration. Unlike Predator, we decided early in the Global Hawk Program that the Air Force would be the operating service. This allowed us to migrate several important lessons learned from the Predator to the Global Hawk Program.

Several organizational structure changes have already been made to improve OSD ISR oversight:

- A new Deputy Assistant Secretary of Defense for C3ISR and Space was

established. This position consolidates and integrates the airborne (manned and unmanned), terrestrial, and overhead resources and efforts. This is the first time we have oversight of all ISR sensors in one office.

- The Intelligence Senior Steering Group was established to provide senior oversight of major intelligence systems requirement development, acquisition, architectures, and related intelligence issues. The ISSG reviews major intelligence systems requirements and architectures, and evaluates those against all intelligence providers and Defense and Intelligence Community tasking, processing, exploitation, and dissemination systems.

13. Spectrum Reallocation

Over the past several years the Congress has received a number of reports regarding significant unanticipated costs that the Department of Defense has incurred, or may incur, as a result of Spectrum re-allocation.

A. What is your estimate of the total potential cost that the Department of Defense would incur if it is forced to redesign its communications equipment in order to allow other non- DOD entities to use these frequencies without regard to the interference they may cause to, or receive from, the Department's equipment?

ANS: It is extremely difficult, if not impossible, to estimate the total potential cost that the Department would incur because each spectrum-dependent system in each individual spectrum band must be analyzed when considering the impacts of interference. As we have indicated in our previous correspondence, to develop good cost estimates, we must know exactly what DoD systems will be affected, whether the system must be modified or replaced, and the characteristics of the non-DoD systems that want to share the band. It is safe to say that the Department has significant investments in spectrum-dependent systems that could require redesign if additional spectrum is reallocated. Furthermore, as technology evolves, the need to track low-observable targets will require more bandwidth (frequency spectrum) – not less – making spectrum reallocation a national security issue.

In DoD's report to Congress in December 1998, we provided a range of cost impacts for the 235 MHz reallocated under the Omnibus Budget Reconciliation Act of 1993 and the Balanced Budget Act of 1997. The ranges of estimates were $247.2M - $1,240.2M for the 1993 Act and $436M - $2,518M for the 1997 Act. Once again, the ranges of costs were provided to account for the complexities and the technical, policy and doctrinal uncertainties.

B. Do you believe it is appropriate for the Department of Defense, and thus the American taxpayers, to incur such costs?

ANS: No. There is an essential need to balance the national security needs of the nation with commercial interests when considering spectrum reallocation. A national blueprint for future spectrum reallocations could mitigate impacts to the Department. For example, if reimbursements of displacement costs were mandated, commercial entities gaining spectrum access would incur the reallocation costs instead of the Department and the American taxpayers.

14. Y2K

The year 2000 is only six months away and the Department has not yet completed all of its renovation and testing to ensure that its computer systems are Y2K compliant. There is considerable concern that noncompliant systems will degrade the Department's capability to execute the National Military Strategy if so required.

Would you please outline the current state of the Department's efforts to renovate its mission essential systems; describe those systems that will not be renovated in time; and the contingency plans the Department has developed to ensure that it can execute the necessary functions.

ANS: The Department's status of system Year 2000 compliance, as of June 11, 1999, is as follows:

- Mission critical systems are 91.3% complete (1,860 of 2,038); by September 30, 1999, over 99% are projected to be complete.
- Non-mission critical systems are 94% complete (4,364 of 4,720); by September 30, 1999, over 99% are projected to be complete.
- Installations are 98.3% complete (626 of 637); all are projected to be complete by July 31, 1999.
- Defense computer megacenters are 89.7% complete (315 of 351); by September 30, 1999, over 95% are projected to be complete.

The status and impact of systems not yet completed is briefed to the Deputy Secretary of Defense in detail at monthly Y2K Steering Committee meetings attended by the DoD Inspector General, the General Accounting Office, and members of congressional committee staffs and the Office of Management and Budget, and John Koskinen, chair of the President's Council on Y2K Conversion. As of June 11, 1999, there are 178 mission critical systems remaining to be completed. In many cases, the systems not yet "complete" are due to the need to install a known fix at many locations. Completion of these systems is affected by operational deployment schedules, such as for Carrier Battle Groups, when the fix will be applied upon return to home port. All mission critical systems are projected to be compliant by December 31, 1999.

DoD is using Contingency Planning to ensure continuity of critical functions in the event of unforeseen disruptions to DoD and Government Systems or the supporting infrastructure. The two types of Y2K continuity and contingency plans within DoD are:

- System Contingency Plans document planned actions associated with a timely restoration of a system to full functionality following a Y2K-related disruption to the hardware and software associated with the system. System Contingency Plans are required for all date-aware mission-critical systems. As of June 11, over 98.7% of system contingency plans are complete and the status is being tracked in the DoD Y2K Database.

- Operational Contingency Plans document planned actions associated with maintaining a pre-designated minimum level of capability during any disruptions to

the supporting systems or infrastructure. Operational Contingency Plans may be written in support of a single system or application, a single mission or function, or the full range of missions or functions performed by a DoD entity. (When the planning is in support of a single system or application, the system contingency planning information and the operational contingency planning information are often combined in a single plan). Operational Contingency Plans are also called Continuity of Operations Plans, Operational Continuity Plans or Business Continuity Plans.

The Department has fixed most of our mission critical systems and is working hard on the remainder. DoD is developing and exercising continuity of operations plans for all key functions and processes. We are preparing the DoD leadership and organizations for Y2K operations and are working with those who rely on DoD and upon whom we rely. Special attention has been placed on nuclear systems and they have already been tested several times. The Department is looking ahead to leverage its Y2K experience for future DoD information technology operations. The Department will be able to execute its national security missions throughout the Y2K transition period.

15. Information Management

In 1995, GAO designated the Department of Defense effort to streamline business operations and deploy more efficient standard information systems as a "high-risk" area, indicating that it was especially vulnerable to waste and mismanagement. Since 1995, GAO has continually reported that the Department of Defense has lacked effective management and oversight controls of the Information Technology (IT) investments. The areas of concern include controls and processes to:

1) ensure that the costs and risks of multimillion dollar projects are justified;
2) monitor progress and performance; and
3) stop projects shown to be cost ineffective or technically flawed.

A significant change in the Department of Defense IT management and oversight process occurred in July 1996 when the Department of Defense disestablished the Major Automated Information Review Council which was the primary body for overseeing major automated information systems and other IT investments.

A. What is the status of efforts to improve the Department of Defense IT oversight process and what actions have you taken to improve information management and oversight controls since being selected as the Department of Defense Chief Information Officer?

ANS: The Integrated Product Team (IPT) process that Secretary Perry implemented in 1995, as part of the Department's overall Acquisition Reform, has enabled us to build successful and balanced programs, identify and resolve issues, and make sound and timely recommendations to facilitate acquisition decision making. We disestablished the MAISRC in 1998 and in its place created an Information Technology Overarching Integrated Product Team. All other acquisition oversight policy and processes remain in effect, and we continue our hands-on oversight via the successful IPT process. As the DoD CIO, I have visibility over 90 major information technology (IT) investments. The CIO has also been named a member of the Defense Resources Board and Program Review Group during my tenure as DoD CIO, and as such the CIO is an integral part of the Department's Planning, Programming and Budgeting System (PPBS) process.

The existing oversight process, however, does not always adequately address the linkage between IT investments and mission outcomes, has a narrow focus on individual systems, and provides extremely limited visibility into the overall state of DoD IT. C3I has been prototyping an information technology investment portfolio oversight process that will address these gaps systematically and comprehensively.

My vision as the DoD CIO is to institutionalize a portfolio approach to managing and overseeing IT investments. This process will ensure that there is a direct linkage between IT investment decisions and DoD mission, warfighter, functional goals and outcomes; processes and systems are compliant with the Clinger-Cohen Act and related reform legislation, and that IT investments result in measurable improvements to DoD mission-related and administrative processes; all in the service of achieving

interoperability across DoD.

The Department of Defense reported on December 1, 1998, to the Defense Committees that the Department recognizes that its current IT management process has the following shortfalls:

1) minimal linkage between IT investments and functional process changes;
2) individual systems narrowly focused on specific functions and organizations rather than mission; and
3) fragmented systems and infrastructure, resulting in a lack of fully integrated and interoperable capabilities.

B. Please comment on each of these problems and explain what the Department of Defense is doing to correct them?

ANS: The implementation within DoD of a structured Information Technology Investment Portfolio process will go a long way to correct these existing deficiencies.

Today, information technology investments are generally managed and overseen in isolation from the functional processes they support. Further, IT investments may be only one factor among many (training, physical infrastructure, personnel accessions, outsourcing) in converting an obsolete process into one that delivers substantial benefits to DoD. If a more holistic management approach to IT's effect on process change is not implemented, an IT investment may in fact be achieving cost, schedule, and benefit goals; yet the mission it is to improve may be failing to achieve its desired outcomes. To overcome this deficiency, a process change portfolio that contains all elements that may influence that change can be organized and managed as a single entity. Under this construct, IT investments pertaining to the process change will be viewed in their proper context: the IT will be managed as an integral part of the "business."

A concurrent problem is that DoD management processes commonly view IT investments in isolation from each other and from the mission outcomes that they support. The Planning, Programming and Budgeting System process forces us to review things by line item, not as IT investments. Once again, organizing these IT investments into portfolios related to achieving specific mission outcomes can be of substantial use in overcoming this deficiency. Such mission-based portfolios of IT investments that implement end-to-end functional or operational processes and achieve specific mission outcomes could do much to insure delivery of required capabilities to the end-user. Organizing IT investments in this manner will also focus finite resources on the essentials of performance, mission outcomes, customers and end-users.

Finally, a continuing problem of our existing management process is fragmented systems and infrastructure. Not viewing systems in the context of the enterprise infrastructure that will be required to support them has led to substantial DoD synchronization problems. Systems may be fielded years before all of their supporting infrastructure may be available. Conversely, infrastructure capacity may be purchased only to sit idle awaiting the deployment of systems that have slipped their deployment

dates. One remedy to this issue is to provide management oversight into developing systems concurrently with their expected infrastructure through the use of portfolio techniques. Portfolios of IT investments managed as a single entity along with their necessary infrastructure requirements may help to ensure that synchronization becomes an issue of the past.

The Clinger-Cohen Act of 1996 introduced requirements emphasizing the need for the Department of Defense to significantly improve management processes, including how it selects and manages IT resources. For instance, a key goal of the Clinger-Cohen Act is that the Department of Defense should have institutionalized processes and information in place to ensure that IT projects are being implemented at acceptable costs, within reasonable timeframes, and are attributing to tangible, observable improvements in mission performance.

C. What is the status of the Department's efforts to implement the Clinger-Cohen Act?

ANS: The Department's approach to implementing the Act has been one that builds on our past successes and seizes the opportunities the Act offers to reinvent and reinvigorate how we deliver information to warfighters and those who support them. Specifically, the Department:

- Issued its Information Management Strategic Plan in March 1997, and is now in the process of updating it to reflect a stronger linkage to the Report of the Quadrennial Defense Review, the Defense Reform Initiative, and Joint Vision 2010.

- Established a new governance substructure that fosters a more collaborative policy-making environment. This substructure uses the DoD CIO Council as DoD's executive management body for improving information and information technology management.

- Issued the Information Technology Investment Management Insight Policy for Acquisition that simplifies and streamlines the way that DoD Components inform the DoD CIO of their information technology acquisitions.

- Uses the PPBS, in conjunction with its requirements and acquisition processes, to ensure that the correct information investments are selected. Changes have been made in the PPBS to ensure full participation of the DoD CIO in the decision making process. In addition, we have convened an Integrated Product Team to make recommendations on institutionalizing a portfolio approach to managing and overseeing information technology (IT) investments that ensures: that there is a direct linkage between IT investment decisions and DoD mission, warfighter/functional goals and outcomes, processes and systems are compliant with the Clinger-Cohen Act and related reform legislation, and IT investments result in measurable improvements to DoD mission-related and administrative processes.

- Initiated actions to manage its worldwide information infrastructure as a coherent Global Networked Information Enterprise (GNIE). The GNIE policy development initiative incorporates change management, advanced technologies, and process re-engineering to move us toward a ubiquitous, secure, available network to support information superiority.

- Established an Enterprise Software Initiative Working Group, which has developed innovative solutions to achieving cost saving through wholesale bulk purchasing and discount pricing of computer software.

- Established a Defense-wide Information Assurance Program to build and sustain a secure information infrastructure. In fact, implementing effective programs for establishing information assurance and critical infrastructure protection is second only to Y2K in the ten goals that have been established to focus our attention on achieving Information Superiority.

- Developed Clinger-Cohen competencies that depict skill requirements and knowledge required by CIOs and information management personnel. Along these same lines, the Department continues to sponsor CIO executive training session for CIOs, Deputy CIOs, and senior managers with CIO responsibilities.

16. Congressional oversight

In order to exercise its legislative and oversight responsibilities it is important that this Committee and other appropriate committees of the Congress are able to receive testimony, briefings, and other communications of information.

A. Do you agree, if confirmed for this high position, to appear before this Committee and other appropriate committees of the Congress?

ANS: Yes

B. Do you agree, when asked, to give your personal views, even if those views differ from the Administration in power?

ANS: Yes

C. Do you agree, if confirmed, to appear before this Committee, or designated members of this Committee, and provide information, subject to appropriate and necessary security protection, with respect to your responsibilities as the Assistant Secretary of Defense for Command, Control, Communications and Intelligence?

ANS: Yes

D. Do you agree to ensure that testimony, briefings and other communications of information are provided to this Committee and its staff and other appropriate committees?

ANS: Yes